IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

BRIDGETREE, INC., a South Carolina company, and TWO BIT DOG, LLC, a South Carolina limited liability company, Plaintiffs v. RED F MARKETING LLC, a North Carolina limited liability company; TARGET POINT, LLC a North Carolina limited liability company; DANIEL ROSELLI, an individual; TENG LI, an individual; JASON LI, an individual; MALI XU, an individual; MARK EPPERLY, an individual; and ELTON T. SCRIPTER, an individual, Defendants.	)	**COMPLAINT** JURY TRIAL DEMANDED

1. Plaintiffs Bridgetree, Inc ("Bridgetree") and Two Bit Dog, LLC ("Two Bit Dog"), a Bridgetree affiliate, bring this Complaint to seek redress for Defendants' data theft, trade secret misappropriation, unlawful access to Bridgetree's computers, and unfair competition.

2. As part of their conspiracy to defraud Plaintiffs and raid Bridgetree's trade secrets, employees, other competitive information and data in order to unlawfully establish a competing enterprise, Defendants violated, among other things, the North Carolina Trade Secrets Protection Act, the Racketeer Influenced and Corrupt

Organizations Act, the Computer Fraud and Abuse Act, and the Digital Millennium Copyright Act.

3. At least as early as the summer of 2009, Defendants entered into a conspiracy to raid certain of Bridgetree's key personnel, confidential information, and trade secrets. This case arises from the overt and covert acts in furtherance of the attempts of Defendants RED F Marketing, LLC ("RED F") and Target Point, LLC ("Target Point") to unlawfully and improperly compete with Plaintiff Bridgetree's business by, *inter alia*, recruiting Bridgetree's former Vice President, Chief Technical Officer, and Chief of Privacy and Security, Defendant Teng Li, and the unlawful misappropriation of various Bridgetree trade secrets and confidential information upon Teng's abrupt departure from Bridgetree. Prior to January 2010, did not offer and had no ability to offer services in competition with Bridgetree. However, Defendants raided Bridgetree to obtain the trade secrets and know-how they did not have the time or resources to develop themselves, and which Bridgetree had spent millions of dollars and more than a decade to develop.

4. In January 2010, Defendants RED F, Target Point, Daniel Roselli ("Roselli"), Mark Epperly ("Epperly"), and Teng Li (collectively "RED F Defendants") revealed for the first time their intention to become a competing concern, using Bridgetree's employees and trade secrets, in order specifically to capitalize on a time sensitive opportunity to secure work from Bridgetree clients including IBM.

5. On January 1, 2010, the RED F Defendants, including Teng Li, then a key Bridgetree employee, met with Defendant Elton Scripter ("Scripter"), an IBM employee, at a local Charlotte restaurant to pursue a "partnership" between the co-conspirators to

win an important IBM project. They planned to win this project using non-public IBM information provided by Scripter and stolen services and know-how from Bridgetree.

6. On January 4, 2010, Teng Li resigned his senior management position with Bridgetree as Bridgetree's Vice President, Chief Technical Officer, and Chief of Privacy and Security, effective the next day, to join RED F as an employee. The same day that Teng Li gave his notice to Bridgetree, January 4th, a substantial portion of Bridgetree's key personnel in Xian, China resigned from Bridgetree to join a newly formed RED F operation in Xian, China, headed by Teng Li.

7. Using Bridgetree's valuable trade secrets and confidential information, the RED F Defendants almost immediately were able to become a competing concern, as their business interests now involve offering services in direct competition with Bridgetree.

8. Since January 4, 2010, Bridgetree has conducted an extensive forensic computer investigation. Based upon this investigation, Plaintiffs have established that RED F's operations in Xian, China were at all relevant times directed by Teng Li and RED F from North Carolina. This operation employed and relied upon Bridgetree technical talent, trade secrets, confidential information and other Bridgetree property without the authorization, approval, knowledge or acquiescence of Bridgetree. The investigation shows that numerous emails and computer files belonging to Bridgetree were deleted from Teng Li's and his Xian subordinate, Jason Li's, Bridgetree-owned computers. These deletions started at least as early as Teng Li's resignation notice on January 4, 2010, and continuing at least until Teng Li belatedly returned his Bridgetree-owned computers to Bridgetree on January 7th, more than two (2) days after Teng Li's resignation from Bridgetree. In addition to the above deletions, Defendant Teng Li and

Xian-based Defendant Jason Li apparently copied a vast amount of proprietary Bridgetree data and trade secrets between January 4th and January 10th. Bridgetree trade secrets were used by Defendants to establish their Xian, China operation and to provide services in the United States which Defendants were unable to provide prior to the arrival of the former Bridgetree employees with stolen Bridgetree know-how and trade secrets.

PARTIES

Plaintiffs

9. Bridgetree is a privately held corporation. It was chartered in North Carolina in 1995 and relocated as a South Carolina corporation in 2009. Bridgetree is substantially owned and controlled by Mark Beck, who serves as the Chief Executive Officer of Bridgetree.

10. Bridgetree provides marketing data, information, analytics and logistics services to many important U.S.-based consumer, retail and business marketers. Such marketing data, information, analytics and logistics services are used by Bridgetree's customers to develop information to achieve better sales results; improve marketing research; modeling; response analysis; forecast consumer purchasing behavior; database construction and maintenance; data gathering, scoring and variable coding for message production; web programming; website and data hosting and maintenance; and on-demand marketing and printing systems.

11. In 2000, Bridgetree started operations in Kolkata, India, and in 2007, Bridgetree opened a facility in Xian, China.

12. Two Bit Dog is a limited liability company that was chartered in North Carolina in 1998. In January 2010, Two Bit Dog relocated to South Carolina and became a South

Carolina limited liability company. Defendant Teng Li is one of two members of Two Bit Dog.

Defendants

13. RED F, a North Carolina limited liability company, and has in the past operated primarily an advertising agency.

14. Daniel Roselli is the President of RED F and resides at 2611 Whitney Hill Road, Charlotte, North Carolina 28226.

15. Teng Li is presently the Chief Technology Officer and Managing Director of RED F. Until January 4, 2010, Teng Li was a senior executive and key Bridgetree employee. Teng Li resides at 12406 Aden Creek Way, Pineville, North Carolina.

16. Jason Li is Bridgetree Xian's former Team Leader and Chinese citizen. As Team Leader, Jason Li supervised all work performed at Bridgetree Xian. Jason Li reported directly to Defendant Teng Li.

17. Mali Xu is Bridgetree Xian's former bookkeeper and office manager and Chinese citizen.

18. Mark Epperly was the Vice President at Vision Marketing until he recently became the President of Target Point. Epperly was previously employed by Bridgetree as a Business Development Manager from 2004 to 2007. Epperly resides at 6917 Club Champion Lane, Mint Hill, North Carolina.

19. Target Point is a North Carolina limited liability company. Target Point was formed by RED F, Roselli, and Epperly to provide another vehicle through which RED F could offer services competitive to Bridgetree. Defendants formed Target Point using Bridgetree's employees and confidential, proprietary and trade secret information.

20. Elton T. Scripter is Advanced Analytics and Optimization Manager of IBM Business Service. Defendant Scripter was previously employed by Bridgetree as a Data Logistics Specialist from 2003 to 2004. Upon information and belief, Scripter's residence is in Charlotte, North Carolina. Scripter's employment address is 8501 IBM Drive, Charlotte, North Carolina 28262-4333.

JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction over this action pursuant to 17 U.S.C. § 1203(a), 18 U.S.C. §§ 1964(a) and 1964(c), and 28 U.S.C. §§ 1331 and 1367.

22. This Court has personal jurisdiction over Defendants consistent with the U.S. Constitution and N.C. Gen Stat. § 1-75.4 because, on information and belief, Defendants are present in this State, regularly and actively conduct business in this State and judicial district, have sufficient minimum contacts with this State, and are subject to the jurisdiction of the Court.

23. Venue is proper in the United States District Court for the Western District of North Carolina pursuant to 28 U.S.C. §§ 1391(b) and (c).

FACTS COMMON TO ALL COUNTS

Bridgetree's Trade Secrets

24. There are multiple kinds of Bridgetree trade secret information which have been stolen by Defendants, specifically including: (1) Pre-mover services know-how and software; (2) print marketing on-demand services know-how; (3) Proprietary information related to Bridgetree customer needs and industries; and (4) information related to how Bridgetree's overseas operations are organized to work with Bridgetree's U.S. operations. Each of these four (4) bundles of Bridgetree trade secret information will be more fully

described below. In addition, Defendants have used non-public information regarding the identities and skills of Bridgetree employees and its client list to which trade secret protection applies under applicable law,

25. Bridgetree's business is based in the United States and is supported by offices in India and China. Bridgetree has spent considerable amounts of time, money and effort in developing its services. The methods by which Bridgetree develops and provides these services are highly confidential and are not generally known outside of Bridgetree or its affiliates. In particular, Bridgetree has invested substantial time and money in developing its foreign offices and its pre-mover and print marketing on-demand services to meet its customers' particular needs. Bridgetree takes reasonable steps to preserve the confidentiality of its sensitive information, and has a written security policy and security procedures to protect such sensitive, confidential and trade secret information from disclosure.

Bridgetree's Pre-Mover Services

26. It is well-known that large numbers of Americans change their residences each year. "Pre-movers" are individuals or households that have been identified as likely to change residences within a relatively short term. Certain purchase behaviors such as home, entertainment, furniture and appliance purchases and other lifestyle changes such as new employment, divorce and marriage are to varying degrees correlated with residence change decisions. Businesses, such as Bridgetree, use various methods to identify pre-movers and compile such information into a usable format ("pre-mover data"). Retailers, marketers and other customers of businesses such as Bridgetree and RED F use pre-mover data to send targeted direct mail or email and other solicitations to

such pre-movers. The greater the accuracy and timeliness of the pre-mover data, the more valuable it is.

27. Bridgetree has a sophisticated, proprietary system that was developed and refined through trial and error over a ten year time period for acquiring, updating and distributing its pre-mover data. This system constitutes a Bridgetree trade secret and has given Bridgetree a marketplace advantage over its competitors. The methods that Bridgetree developed and uses are not generally known in the industry, and could not independently be developed by a potential competitor without great expense, and substantial research and development requiring years of effort..

28. Bridgetree supported its pre-mover business using employees and software in the United States and Bridgetree's Xian office. Bridgetree employees in the Xian office were the keepers of the source code integral to Bridgetree's pre-mover software capabilities.

Bridgetree's Print Marketing On-Demand Services

29. Marketers desire to send print marketing materials targeted to specific customers rather than untargeted mass mailings. Typically, the marketer will develop print marketing materials and take the copy along with a list of their targeted customers to a printer to be printed. This requires the marketer to work with the printer to customize the marketing materials for each targeted customer. This process takes time, money and is particular to each printer; thus the marketer is wed to a specific printer for each marketing campaign.

30. Bridgetree has developed a custom print marketing on-demand system whereby its clients can select certain parameters from a database of the client's target customers to meet their marketing objectives. Bridgetree's system then merges the target customer's

information into the marketing materials to produce a ready to print file in a format that can be loaded into any printer's machines without the printer having to manipulate the file. Bridgetree's system enables marketers to switch printers and formats with little cost. This effectively turns printing into a commodity whereby marketers are able to substantially lower their printing costs and increase quality through competition among printers. Bridgetree's print marketing on-demand system also can generate finished materials for email and telephone marketing campaigns in much the same way, providing similar benefits to its clients.

31. Bridgetree's print marketing on-demand system was developed and refined through trial and error over a number of years, drawing upon Beck's unique knowledge of both the printing business and electronic data business. This system constitutes a Bridgetree trade secret and has given Bridgetree a marketplace advantage over its competitors. The methods that Bridgetree developed and uses are not generally known in the industry, and could not independently be developed by a potential competitor without great expense, and substantial research and development requiring years of effort..

32. Bridgetree supported its print marketing on-demand system using employees and software in the United States and Bridgetree's Xian office.

Bridgetree's Confidential Customer, Employee and Vendor Information

33. Bridgetree does not publicly disclose the names of its customers, employees or vendor identities; scope and details of work performed for its customers; or other customer information such as marketing objectives and competitive advantages. Over a number of years, Bridgetree has acquired valuable information regarding the particular requirements of its customers and their industries and how to best meet these

requirements. Bridgetree's knowledge of such customer requirements is not generally known in the industry and constitutes a Bridgetree trade secret which gives Bridgetree a marketplace advantage over its competitors. Such information could not independently be developed by a potential competitor without great expense, and substantial research and development requiring years of effort..

Bridgetree's Foreign Operations

34. In 2000, Bridgetree started operations in Kolkata, India. Through substantial cost and effort, Bridgetree developed processes and procedures to make its Kolkata operation successful and fully integrated with its U.S.-based operations and to seamlessly service its U.S. customers ("Integration Procedures"). The Integration Procedures developed by Bridgetree are not generally known or readily ascertainable. These confidential processes and procedures constitute a Bridgetree trade secret.

35. In 2007, Bridgetree opened a facility in Xian, China ("Bridgetree Xian") to support its U.S.-based operations using its Integration Procedures. The Integration Procedures allowed Bridgetree to expedite the opening and profitability of Bridgetree Xian. From 2007 until his departure to RED F, Defendant Teng Li directed the Bridgetree Xian operations.

Bridgetree's Copyright-Protected Works and Technological Measures to Prevent Unauthorized Access

36. The National Consumer Database is the largest, most comprehensive marketing database in the U.S., and is a key component to Bridgetree's pre-mover system.

37. Bridgetree pays substantial licensing fees for access to data in the National Consumer Database, which data is not freely available otherwise.

38. Bridgetree takes the data received from the National Consumer Database and analyzes, edits and adds to the data, thus creating its own custom version of the database ("Bridgetree National Database").

39. The Bridgetree National Database resides on a server hosted by a third party. A small, designated number of Bridgetree employees can access the Bridgetree National Database data, which is accomplished in two ways. One means of access is through a custom web interface designed by Bridgetree. The second is by logging directly onto the third party server and bypassing Bridgetree's interface.

40. Both methods of access to the Bridgetree National Database require the user to enter a valid username and password to log onto the respective system. Moreover, each system maintains a log documenting each entry into the system by username.

Teng Li and Jason Li at Bridgetree

41. Upon information and belief, Defendant Teng Li is an American citizen who holds a Ph.D. in statistics from the University of Maryland Baltimore County. Teng Li was hired by Bridgetree in 2003 as head of security. In 2005, Teng Li was promoted to Vice President, Web and Data Systems. In June 2009, Teng Li became Bridgetree's Vice President, Chief Technical Officer, and Chief of Privacy and Security.

42. As Bridgetree's Vice President, Chief Technical Officer, and Chief of Privacy and Security, Defendant Teng Li had substantial dominion and control over Bridgetree's operations and had access to Bridgetree's trade secrets. Beck was the only person senior to Teng Li at Bridgetree. He relied on Teng Li's technical expertise and placed trust and confidence in Teng Li's abilities.

43. In 2009, and in other years, Teng Li was the highest paid Bridgetree employee apart from Beck. It was well known within and outside Bridgetree that Teng Li was the heir apparent to Beck in control of the day to day operation of the business. In fact, there was a procedure for transferring complete control over Bridgetree's operations to Teng Li in the event of Beck's incapacity.

44. Teng Li routinely made and independently executed significant decisions important to Bridgetree's business. For example, Teng Li was able, without securing advance approval from Beck, to assign or move key Bridgetree employees to or from particular projects including Bridgetree's pre-mover activities.

45. As Bridgetree's Chief Technical Officer, Teng Li, in the course and scope of his employment with and on behalf of Bridgetree, was the main architect of Bridgetree's technical and communications infrastructure. Teng Li controlled all of Bridgetree's information technology systems. In addition to Mark Beck, Teng Li was the only Bridgetree employee with full and complete access to all of Bridgetree's information and information technology, including but not limited to, Bridgetree's passwords, business methods, hardware configuration, custom applications, customer lists, and operating information.

46. Teng Li designed Bridgetree's information technology system so that Bridgetree employee emails and Bridgetree confidential and trade secret data were maintained on Bridgetree employees' company-owned personal computers, not on a centralized server. Further, Teng Li designed the system such that the information on the company-owned personal computers was not routinely backed up on other computers. Thus, for a given employee of Bridgetree, the individual employee's laptop computer was the sole source

of much of their Bridgetree data and email. Bridgetree's servers contained databases, but many of the executable programs resided on individual computers.

47. As Chief of Privacy and Security, Teng Li was responsible for developing and implementing Bridgetree's security policy. For example, Teng Li created the security policies that required Bridgetree employees to have need-to-know access to Bridgetree servers and files. Teng Li was responsible for conducting security audits and implementing security procedures as required by law and Bridgetree's customers.

48. Teng Li owed a legal duty to Bridgetree to keep confidential, and not to use or disclose, Bridgetree's confidential, proprietary and trade secret information and data outside of Bridgetree's business. This information and data included the requirements of Bridgetree's customers, the identity and employment particulars of Bridgetree's employees, Bridgetree's passwords, business methods, hardware configuration, custom applications, customer lists, customer requirements and operating information. Particularly, Teng Li knew the value and confidential nature of Bridgetree's pre-mover services and print marketing on-demand services. Teng Li further knew which Bridgetree employees were responsible for maintaining these systems and had access to the pre-mover and print marketing on-demand source code and technical components.

49. Jason Li was hired by Bridgetree Xian in June 2007 as Team Leader in Bridgetree Xian. As Team Leader, Jason Li supervised all work performed at Bridgetree Xian. Jason Li reported directly to Defendant Teng Li.

Defendants' Unlawful Activities

50. Prior to January 2010, RED F did not offer data mining, pre-mover or print marketing on-demand services that competed with Bridgetree, and RED F had no

facilities in China. Envious of Bridgetree's success and unable or unwilling to lawfully develop a competing business without misappropriating Bridgetree's assets, Defendants conspired to raid certain of Bridgetree's key personnel, confidential information and trade secrets.

51. Although the precise dates are presently unknown, upon information and belief, the conspiracy and planning for the raid began at least as early as mid to late 2009. On August 24, 2009, Articles of Incorporation for the RED F affiliate, Target Point, were filed with the State of North Carolina. That same date, Epperly contacted Mark Beck to arrange a meeting among Epperly, Beck, and Roselli. As a former Bridgetree sales person, Epperly was aware of the value of Bridgetree's capabilities and key personnel. In addition, until recently, Epperly was a Vice President and sales executive for Vision Marketing. Vision Marketing was a Bridgetree licensee and re-seller of Bridgetree's pre-mover data. As such, and subject to confidentiality obligations, Vision Marketing had limited access to certain confidential aspects of Bridgetree's trade secret pre-mover program. After the raid, Vision Marketing ceased to be a Bridgetree customer, ostensibly because they no longer had a need for Bridgetree's pre-mover data.

52. On August 28, 2009, Beck, Roselli, and Epperly met over lunch at Bricktops, a Charlotte, North Carolina restaurant. At this lunch, the parties discussed the general nature of their businesses, including Bridgetree's pre-mover and print marketing on-demand capabilities, with the understanding, at least to Beck, that the parties might be able to work collaboratively in the future. Beck did not knowingly disclose any of Bridgetree's confidential information or trade secrets at this lunch meeting. Upon information and belief, the real, and undisclosed, purpose of this meeting was for Roselli

and Epperly, in furtherance of their conspiracy, to gain information about Bridgetree's operations and to assist with their new venture, Target Point, which they planned to use to compete with Bridgetree. At no time did Epperly or Roselli advise Beck that they planned to offer pre-mover or print marketing on-demand services in competition with Bridgetree.

53. Upon information and belief, later in August or September 2009, Epperly set up a golf meeting between Defendants Roselli and Teng Li.

54. In the last quarter of 2009, Teng Li uncharacteristically began to miss customer deadlines and neglected his duties at Bridgetree and at Two Bit Dog.

55. On November 17, 2009, Teng Li met with RED F's CEO, Sara Garces, to discuss the work he would do for RED F, and the market value of such work.

56. Upon information and belief, Roselli and Epperly thereafter told Teng Li that IBM had a substantial need for services that RED F might provide if Teng Li could help RED F in performing those services. Defendant Scripter, who had known Teng Li since Scripter's previous employment at Bridgetree, had recently joined IBM. Upon information and belief, Scripter's IBM duties included making recommendations to vendors to work with IBM and its customers. At that time, IBM was seeking competitive bids for services of the type provided by Bridgetree. Defendants knew that RED F and Target Point had no current capability to win the IBM work, and that to compete for the IBM business, Bridgetree trade secrets and Xian resources were needed. Also, Teng Li was needed to ensure RED F's ability to lure top Bridgetree Xian employees to establish RED F's Xian, China office, which would thereby provide technical knowhow missing from RED F.

57. On January 1, 2010, Roselli, Epperly, Scripter, and Teng Li met secretly at a restaurant in Charlotte, North Carolina to discuss how to prepare a winning bid to IBM for the work on which Teng Li and the Xian personnel were essential. At that meeting, all these individuals discussed their "partnership" and how to conceal the "partners'" identities and relationship while discussing the potential work with IBM officials other than Scripter. In addition, Scripter knowingly and deliberately revealed to the "partners" the specific firms that were competing with RED F for the work from IBM. Notably, to conceal his deception, Scripter did not use his IBM email account to disclose this information, rather, a private Google Gmail email account was used. This information was useful to Defendants because it enabled the "partners" to differentiate RED F's offering from the competition and enabled Teng Li to know which of Bridgetree's property and Xian personnel to raid. The RED F Defendants would not have had this information without Scripter's improper disclosure of confidential IBM information to the other Defendants.

58. The result of this meeting and Scripter's improper disclosure of the IBM bid information to the RED F Defendants was that the Defendants learned they had to act immediately to create new capabilities at RED F and Target Point to be successful in winning and performing the IBM project they sought. Teng Li conspired with the others in their plan to raid Bridgetree's trade secrets and personnel.

59. As a result, while still employed by Bridgetree and using Bridgetree's confidential information, Teng Li actively recruited Bridgetree Xian employees to join RED F. RED F did not have access to the identity of the Bridgetree Xian employees or other Chinese individuals with comparable skill sets without Teng Li's disclosure of

Bridgetree's confidential information. Moreover, to induce them the join RED F, Teng Li and others under his supervision and control, upon information and belief, falsely communicated to Bridgetree Xian employees that Bridgetree Xian was closing, thus causing them to believe that they could not remain employed by Bridgetree.

60. On January 4th at 8:47 a.m., Eastern Standard Time (which corresponded to approximately 9:47 p.m. Xian time on January 4th), Teng Li called Beck and resigned from Bridgetree. Teng Li stated that he would work through the business day of January 5th and thereafter he would consult for Bridgetree for a consulting rate of $150 per hour.

61. Although Teng Li resigned from Bridgetree on January 4, 2010, he wrongfully retained certain Bridgetree property provided to him by the company during his employment, including two laptop computers. These laptop computers were used in interstate commerce and contained Bridgetree confidential and trade secret information used in interstate commerce pertaining to Bridgetree and Bridgetree Xian.

62. Beginning on January 4th, Teng Li connected multiple electronic storage devices to his laptop and accessed many Bridgetree project folders containing Bridgetree confidential, trade secret, proprietary, and sensitive information. These electronic storage devices contained specific manufacturer, model, and serial numbers known to Plaintiffs as a result of their forensic investigation. Certain of the project folders accessed by Teng Li contained data and programs that were not related to Teng Li's former duties; Teng Li had no legitimate reason to possess or view these folders, especially after resigning from Bridgetree.

63. Upon information and belief, beginning on January 4th and continuing for several days thereafter, Teng Li copied thousands of files containing Bridgetree

confidential, trade secret, proprietary and sensitive information to such personal electronic storage devices or to other locations such as online storage. There was no legitimate purpose for Teng Li to copy, retain possession of or transfer Bridgetree's files in this manner.

64. After Teng Li's January 4th call to Beck, Teng Li would not respond to repeated attempts by Beck and other Bridgetree employees to contact him seeking answers to questions about missing passwords and other important Bridgetree work-related matters.

65. January 5th in Xian, China, the first day after Teng Li's resignation the previous evening, seventeen (17) Bridgetree Xian employees did not show up for work at Bridgetree Xian, including, among others, Defendant Mali Xu, Bridgetree Xian's bookkeeper and office manager. Upon information and belief, these Bridgetree Xian employees left Bridgetree to join RED F in China. Five of the Bridgetree Xian employees who left to join RED F were keepers of and had access to Bridgetree's pre-mover related source code.

66. When departing Bridgetree Xian for RED F, Mali Xu took Bridgetree Xian's accounting books and ledgers containing Bridgetree's confidential information without permission. To this day, despite demands by Bridgetree, Mali Xu refuses to return Bridgetree Xian's accounting books and ledgers to Bridgetree.

67. In addition, Mali Xu took a personal computer belonging to Bridgetree when departing Bridgetree Xian for RED F. To date, Mali Xu has also failed to return this personal computer to Bridgetree.

68. Among those Bridgetree Xian employees who left for RED F was Defendant Jason Li. Upon information and belief, beginning on January 4th and continuing for

several days thereafter, Jason Li, under the direction of Defendant Teng Li and RED F, copied files containing Bridgetree confidential, trade secret, proprietary and sensitive information to personal electronic storage devices or to other locations such as online storage. Included in the files copied were the employment contracts and other human relations documents pertaining to Bridgetree Xian employees. There was no legitimate purpose for Jason Li to copy, retain possession of, or transfer Bridgetree's files in this manner.

69. As stated above, Defendant Teng Li used Bridgetree confidential information and trade secret information, including, for example, salary information, job duty, and technical capability information to target the employees taken to RED F. The RED F Defendants, including Teng Li and others, used this information to improperly induce the targeted Bridgetree Xian employees to join RED F's China venture.

70. At least by January 10, 2010, RED F began operations in Xian, China, in an office one block from Bridgetree Xian's facility. Mali Xu and the other former Bridgetree Xian employees went to work for RED F in its Xian, China office.

71. Upon information and belief, Mali Xu, under the direction of Defendant Li, falsely told Chinese government officials that Bridgetree was moving its operations out of Xian.

72. On January 7, 2010, Defendant Teng Li returned his computers and phone to Bridgetree. At that time, deleted from Teng Li's computer was critical Bridgetree confidential, trade secret, proprietary and sensitive data, including work product and other data belonging to Bridgetree. In particular, Teng Li's computers were missing

critical email communications with Bridgetree customers relating to pending and ongoing business matters.

73. Teng Li knew this deleted information was Bridgetree's property and had great commercial value. Nevertheless, Teng Li apparently copied, removed, or deleted this information from his Bridgetree computers before returning them to Bridgetree more than two (2) days after his resignation from Bridgetree.

74. The deleted data appears to have been deliberately and maliciously deleted by Teng Li. Evidence of these facts was uncovered by extensive computer forensic investigation commissioned by Bridgetree. There is no legitimate or lawful reason for Teng Li to have engaged in such activities.

The Fruit of Defendants' Unlawful Activities

75. On January 20, 2010, RED F announced that it opened an office in Xian, China with 20 employees, primarily, if not exclusively, former Bridgetree Xian employees.

76. RED F stated, "[t]he Xian office will be used for technology projects, including the development of web sites, marketing databases and other online systems." Roselli further stated that "[t]his is a true game changer for our digital marketing-services technologies platform. . . . This greatly increases our competitive advantage in the marketplace as it increases our full spectrum of marketing support for clients."

77. RED F and Target Point did not offer pre-mover or print marketing on-demand services until after Teng Li joined RED F.

78. In a January 20, 2010 *Mecklenburg Times* article, Roselli and Ms. Garces, RED F's CEO, explained that Defendant Teng Li provided the information that allowed RED F

to more quickly establish its Xian office than it otherwise could have. The article states (emphasis added):

> The [RED F] China office will focus on technology-driven projects, such as the development of Web sites and systems, integrated marketing communication portals, and customer marketing analytical tools.
>
> **President Dan Roselli explained that the international opportunity arose after RED F hired Teng Li as managing director and chief technology officer.**
>
> Li is from the town in China where the new office is located, and his **connections** and **industry expertise** helped **simplify** the process of establishing an international presence, Roselli said.
>
> "The whole process has been very interesting," Garces said. "We've gotten up to speed **very quickly** with China labor laws, finances and the legal system. Fortunately, we've had some **help in navigating the waters**."

Sam Boykin, *RED F marketing firm expands into China*, MECKLENBURG TIMES, Jan. 20, 2010 (emphasis added).

79. Since at least January 20, 2010, RED F has been a direct competitor of Bridgetree.

80. Upon information and belief, Target Point also is in direct competition with Bridgetree.

Defendants' Circumvention of the Technological Measures Controlling Access to Bridgetree's Copyright-Protected Works

81. Upon information and belief, even after his resignation, Defendant Teng Li, on behalf of the RED F Defendants, accessed Bridgetree's computer systems, trade secrets and confidential information wrongfully and without permission to unlawfully compete

with Bridgetree, particularly with respect to pre-mover services and print marketing on-demand services.

82. On January 10, 2010, Abel Henson, a Bridgetree employee, entered the Bridgetree's National Database interface as a duly-authorized administrator and disabled Defendant Teng Li's access to the interface, given Teng Li's recent resignation from Bridgetree. Henson then logged off and logged back on to confirm that Teng Li's access had indeed been disabled.

83. On April 12, 2010, Henson discovered that Teng Li's access to the Bridgetree National Database interface had been restored. In addition, Henson discovered that the Bridgetree's National Database interface log files have been erased in an apparent attempt to cover up the restoration of Teng Li's access. But for their deletion, these log files would have recorded Henson's disabling of Teng Li's access and its subsequent restoration. The log would also have reflected actual access to and uses of the database using Bridgetree's protected account.

84. Upon information and belief, Defendant Li, or someone acting under his direction or control, has continued to hack into the Bridgetree National Database on behalf of or for the benefit of the RED F Defendants, through improper circumvention of the technological measures designed to prevent access thereto, and as a result, has been improperly accessing the Bridgetree National Database and utilizing Bridgetree's license to the National Customer Database without authorization or approval.

85. Bob Yuan was a Bridgetree Xian employee who left Bridgetree on January 5, 2010, to join RED F. Bob Yuan and Teng Li worked together to develop Bridgetree's

National Database systems. Bob Yuan utilized the username "bob" when logging on to the Bridgetree National Database server and the Bridgetree National Database interface.

86. In January and February 2010, after Bob Yuan departed Bridgetree for RED F, the user name "bob" logged into the Bridgetree National Database server multiple times.

87. Upon information and belief, Bob Yuan, or someone acting under his direction or control, has been hacking into the Bridgetree National Database server on behalf of or for the benefit of the RED F Defendants, through improper circumvention of the technological measures designed to prevent access thereto, and as a result, has been improperly accessing the Bridgetree National Database and utilizing Bridgetree's license to the National Customer Database without authorization or approval.

Defendants' Racketeering Conduct

88. Defendants Roselli, Epperly, Teng Li, Scripter, Mali Xu, and Jason Li formed a conspiracy to defraud Bridgetree Roselli, Epperly, Teng Li, Scripter, Mali Xu, and Jason Li all stand to benefit personally from their fraudulent activities.

89. Upon information and belief, Roselli left the employ of Bank of America and became an employee of RED F about mid 2005. Later in 2005, Roselli acquired RED F from its founders, Richard Elias and Daniel Feldstein. Upon information and belief, since shortly after Roselli's acquisition of RED F, Roselli desired to improve the profitability of RED F by acquiring Bridgetree's print marketing-on-demand, pre-mover and other capabilities including Bridgetree's capabilities in China.

90. Upon information and belief, Roselli knew that it would require considerable capital and take years to develop such capabilities. The quickest way for Roselli to develop Bridgetree-like capabilities was to raid Bridgetree. To accomplish this objective,

Roselli needed the assistance of people inside and outside of Bridgetree with knowledge of Bridgetree's operations and trade secrets in order to get the required information and capabilities out of Bridgetree.

91. Although the precise dates are presently unknown, upon information and belief, the conspiracy and planning for the raid began at least as early as mid to late 2008 when with the assistance of Mark Epperly, a former Bridgetree sales executive, Roselli and RED F began to offer a print marketing on-demand type service with the assistance of Shutterfly, a national printing firm with a manufacturing location in Charlotte.

92. On April 7, 2009, Epperly sent Beck an email attempting to set up a meeting between Roselli and Beck. Epperly enticed Beck to attend such a meeting by purporting to state that Roselli "has a tremendous amount of respect for [Beck] and what [Beck has] been able to accomplish." Upon information and belief, the real and undisclosed purpose for arranging this meeting was to gain confidential information from Bridgetree regarding how to make RED F's unprofitable Shutterfly operation profitable like Bridgetree's print marketing on-demand system.

93. At least as early as June 2009, Roselli or Epperly or both had recruitment conversations with Teng Li that caused him to focus on RED F and to bookmark RED F's website in his Bridgetree computer. Upon information and belief, Li then began regular email and phone communications with Roselli and Epperly respecting, among other matters, that Li would join them at RED F.

94. On August 24, 2009, Articles of Incorporation for the RED F affiliate, Target Point, were filed with the State of North Carolina. Target Point is a Defendant herein. That same date, Epperly again contacted Mark Beck via telephone to arrange and confirm

via email a lunch meeting among Epperly, Roselli, and Beck. As a former Bridgetree sales person, Epperly was aware of the value of Bridgetree's capabilities and key personnel, in particular Teng Li. Epperly and Roselli realized that if Beck knew they were recruiting Teng Li, he would never agree to meet with them. Although the ostensible purpose of the meeting was to explore ways that RED F and Bridgetree could work together, this objective was never Roselli's or Epperly's true purpose. Rather, they wished to confirm that Beck did not realize that Teng Li was cooperating with their plan to raid Bridgetree.

95. On October 23, 2009, the domain name *targetpoint.us* was registered with godaddy.com by Anne Bradley, RED F's Chief Financial Officer and an agent of Roselli, using interstate communications to further the fraudulent scheme.

96. Upon information and belief, later in August or September 2009, Epperly set up a golf meeting between Defendants Roselli and Teng Li.

97. Upon information and belief, in late October, 2009 Roselli and Epperly enlisted Scripter who knew the value and confidential nature of Bridgetree's trade secrets, personnel, and confidential information. Scripter at that time had recently joined the IBM Corporation in a capacity that enabled him to steer work to RED F.

98. Upon information and belief, Epperly, Scripter, and Roselli knew that Bridgetree would not voluntarily divulge its trade secrets and confidential information or allow an employee to remove those trade secrets from Bridgetree. Upon information and belief, Epperly, Scripter, and Roselli contacted Teng Li after Scripter joined IBM to use the possibility of gaining IBM work to provide an incentive and inducement to Teng Li to

leave Bridgetree and to conspire to, and to steal Bridgetree's trade secrets and confidential information and raid Bridgetree's employees.

99. On November 17, 2009, Teng Li sent an email to RED F's CEO, Sara Garces, regarding the market value to RED F and its current and potential customers of the capabilities and knowledge Teng Li could provide RED F. Bridgetree's trade secrets, confidential information, and employees were integral to this market value.

100. On December 28, 2009, Scripter sent Epperly and Roselli an email regarding RED F bidding for certain IBM work which they knew could be performed by RED F only if and when it received the fruits of its conspiracy to misappropriate Bridgetree's trade secrets, personnel, and confidential information.

101. On December 30, 2009, Epperly sent Roselli and Scripter an email regarding their participation in an interstate teleconference conference regarding the IBM work. Upon information and belief, the IBM work was for a large IBM customer.

102. On December 31, 2009, Scripter, Roselli, Li, Epperly and others working for RED F participated in a teleconference with a New Jersey call-in number, in which they discussed bidding on the IBM work. An earlier email among the parties evidences the concerted effort to hide their conspiracy, by confirming their agreement not to reveal their actual identities during this teleconference and to use first names only.

103. On Friday, January 1, 2010, Roselli, Epperly, Scripter, and Teng Li met secretly at a restaurant in Charlotte, North Carolina, to discuss how to prepare a winning bid to IBM for the work on which Teng Li and the Xian personnel were essential. In an email organizing this meeting, Epperly, then an employee at Vision Marketing, referred

to himself as President of Target Point and described the relationship of the parties as "partners."

104. Upon information and belief, as a result of the January 1, 2010 meeting and while still employed by Bridgetree and using Bridgetree's confidential information, Teng Li used international communications to actively recruit Jason Li, Mali Xu, and other Bridgetree Xian employees to join RED F from at least January 1, 2010 until at least January 5th. It is presently unknown whether these recruitment efforts began earlier in 2009. However, international communications were used to accomplish this recruitment as Teng Li was physically present in North Carolina during most of late 2009 and early 2010.

105. Upon information and belief, Teng Li used international communications to induce Bridgetree employees to join RED F by falsely communicating or causing Mali Xu or Jason Li or both to falsely state to the Bridgetree Xian employees coveted by Teng Li, Roselli, Epperly, Scripter, RED F and Target Point that Bridgetree Xian was closing. This knowingly false and malicious communication was intended to and did cause these employees to believe that they could not remain employed by Bridgetree.

106. Upon information and belief, in late 2009, Teng Li, while present in the United States, contacted Jason Li and Mali Xu in China at numerous times via email and voice communications to enlist them in the conspiracy with Roselli, Scripter and Epperly to steal Bridgetree's trade secrets, confidential information, and employees.

107. Upon information and belief, starting at least as early as January 2010, Teng Li, has been in regular communication with Jason Li and Mali Xu in China in order to coordinate which specific Bridgetree Xian key employees to poach for RED F, all of

whom who had regular trusted access to the Bridgetree trade secrets and confidential information that Defendants needed. Teng Li, Mali Xu, and Jason Li also discussed the compensation that would need to be paid to those individuals once they left Bridgetree and were working on behalf of RED F.

108. Upon information and belief, at least as early as January 2010 and continuing since then, the U.S.-based Teng Li has been in regular communication with Jason Li and Mali Xu in order to establish the RED F facility in Xian, China, which is continuing to exploit Bridgetree's trade secrets and confidential information.

109. On January 4th at 8:47 a.m. EST, Teng Li called Beck and resigned from Bridgetree.

110. Defendants continue to remotely enter Bridgetree's systems in order to steal valuable information. These remote entries take place from IP addresses in China.

111. Defendants Jason Li and Mali Xu ran the technical and administrative aspects of Bridgetree's Xian office from Xian, China. Jason Li and Mali Xu also set up RED F's Xian office from China in coordination with Teng Li who was located in North Carolina. This arrangement necessitated extensive communication between China and the United States all in furtherance of the conspiracy to defraud Bridgetree.

112. On January 11, 2010 at 11:06 p.m., Jason Li sent an email to Yong Cai, a current Bridgetree employee, attaching a copy of a Bridgetree Xian employment agreement. This employment agreement was altered and not the actual agreement. Jason Li's email of the altered agreement was in furtherance of Defendant's' fraudulent conspiracy. Upon information and belief, Jason Li or Mali Xu or both of them used international communications to delete accurate copies of the employment contracts of

the targeted employees from Bridgetree computers located in China and in North Carolina.

113. On January 13, 2010, while in New York, Scripter, called Beck's North Carolina phone number attempting to contact Beck. Beck was not available to receive the call so Scripter left a message on Beck's voicemail. In the voice message, Scripter assured Beck he had nothing to do with Teng Li's departure from Bridgetree and RED F. This representation, an apparent effort to cover up Scripter participation in the conspiracy, was false as evidenced by Scripter's emails of January 1, 2010 to Teng Li (while Teng Li was still a Bridgetree employee) regarding a "partnership" to bid on an IBM project with Roselli and Epperly.

114. On February 4, 2010, at 8:10 p.m., Defendant Mali Xu sent Karen Worley, a current Bridgetree employee in North Carolina, and Yong Cai, a current Bridgetree employee, an email requesting an answer to her prior demand for a release of liability in exchange for returning Bridgetree's ledgers. This communication was done in furtherance of the conspiracy and to cover up the Defendants' wrongdoing.

115. Defendant Teng Li, together with others acting pursuant to the conspiracy and the scheme discussed above, made, sent, and caused to be sent to Bridgetree numerous misrepresentations and omissions in the form of electronic mail and telephone calls, in interstate and/or foreign commerce, with the intent to deceive Bridgetree.

116. Defendants, acting pursuant to the conspiracy and the scheme to defraud discussed above, made, sent, and caused to be sent to each other numerous writings and communications in the form of electronic mail and telephone calls, in interstate and foreign commerce, in furtherance of the conspiracy and the scheme.

117. Defendants have engaged and are engaged in a pattern of criminal conduct, given their past and ongoing use of interstate and foreign wires for the purpose of executing their scheme to defraud Plaintiffs and steal Bridgetree's trade secrets. The existence of this pattern of fraudulent and criminal conduct is evidenced by Defendants' initial conspiracy to raid Bridgetree's trade secrets and confidential data; Defendants' subsequent multiple thefts of Bridgetree's trade secrets and confidential data by Defendant Teng Li and those acting in concert with him; Defendants' further subsequent unauthorized access to Bridgetree's National Consumer Database interface; and Defendants' further subsequent use of Bridgetree's trade secrets and wrongfully acquired data competitively against Bridgetree. In furtherance of each of these activities and Defendants' overall scheme to defraud, Defendants made, sent, and caused to be sent to each other numerous writings and communications in the form of electronic mail and telephone calls, in interstate and foreign commerce.

118. Upon information and belief, Defendants, acting with the intent to defraud Plaintiffs and misappropriate and convert Bridgetree's trade secrets and tangible property, deceived Plaintiffs, and have wrongfully misappropriated and converted Bridgetree's trade secrets and tangible property to their own benefit, are engaged in a continuing enterprise, and are likely to continue that enterprise through the ongoing and future dissemination and use of Bridgetree's trade secrets.

The Harm to Bridgetree Resulting from Defendants' Actions

119. Bridgetree has been harmed by, and incurred considerable expenses as a result of Defendants' unlawful actions, including the looting of Bridgetree Xian's key

personnel, Teng Li's destruction and misappropriation of Bridgetree's property and information, and the recent unlawful access to Bridgetree's database account.

120. Among the files deleted by Teng Li were Bridgetree email files showing his communication with RED F, Roselli, Garces, Scripter, and Epperly. By Teng Li's own design, emails did not reside on other computers at Bridgetree, although normally such emails would be maintained on a server designed to archive email information. Thus, Teng Li believed or hoped that by deleting the emails from his computer they were forever deleted. Additionally, Teng Li believed by deleting or attempting to delete these emails, Bridgetree would be hindered in its ability to follow-up and correct the effects of his misconduct.

121. Since his resignation, Teng Li has not cooperated with Bridgetree in restoring data or providing passwords and other critical information for the continued operation of Bridgetree's business, to which only he had access.

122. At considerable expense and effort, Bridgetree used sophisticated software and professional computer forensics services to recover Teng Li's passwords and to restore certain deleted data from Teng Li's computer. Included in the restored data were customer security discussion reports and action plans prepared by Teng Li at the request of Bridgetree's customers. These reports and action plans were provided to customers by Teng Li and obligated Bridgetree to meet certain customer requirements. Without knowledge of these reports and action plans, Bridgetree would fail to meet customer expectations to deliver on critical aspects requirements. Such failures would likely cause damage to Bridgetree's customers and jeopardize Bridgetree's ability to provide further work to these important customers. Teng Li was the only Bridgetree employee who

knew of the existence of these security reports and action plans and, but for the forensic reconstruction of same, would have been forever lost to Bridgetree.

123. Teng Li did not alert any Bridgetree employees to the existence of these security reports and action plans and, upon information and belief, intentionally deleted them to make them unavailable to Bridgetree.

124. The security reports and action plans are an integral part of Bridgetree's relationship with its clients. Teng Li's concealment and deletion of the security reports has harmed Bridgetree.

125. Upon his resignation from Bridgetree, Teng Li ceased to provide any services to Bridgetree or to make available necessary information such as passwords, work actions needed to be done, or other steps necessary for Bridgetree to provide on-going quality services to its customers. Teng Li intentionally concealed certain undertakings he had made on behalf of Bridgetree to its clients, compromising Bridgetree's ability to provide desired services to such clients.

126. Teng Li's raid of seventeen Bridgetree employees who were integral to Bridgetree's pre-mover and print marketing on-demand systems harmed Bridgetree's ability to service existing customers.

127. As a result of Defendants' actions, Bridgetree has lost Vision Marketing as a customer of Bridgetree's pre-mover services.

128. Defendants' unauthorized access to the National Consumer Database is contrary to Bridgetree's license with the National Consumer Database and has harmed Bridgetree and increased Bridgetree's usage costs.

The Harm to Two Bit Dog Resulting from Teng Li's Actions

129. On account of Teng Li's position of trust within Bridgetree, Teng Li was invited to invest and became a partner in Bridgetree affiliated e-commerce business opportunities, including Two Bit Dog, LLC, a website-based marketer of pet products, www.twobitdog.com and another such entity, Cartoon Networks, LLC.

130. Upon his resignation from Bridgetree and earlier, Teng Li ceased to provide effective services to Two Bit Dog.

131. Two Bit Dog is dependent on Bridgetree for its services. Teng Li's deliberate disruption of Bridgetree's operations and his looting of key Bridgetree Xian technical leaders caused harm to Two Bit Dog and harmed Two Bit Dog's ability to provide on-going quality services its customers.

132. Teng Li's conduct in ceasing to provide effective service to Two Bit Dog breached his fiduciary duty to Two Bit Dog resulting from his ownership interest in Two Bit Dog.

133. As a consequence, Two Bit Dog's relations with its customers and key vendors were materially injured. Thus, Two Bit Dog, LLC suffered a marketing, financial and business relationship loss in 2009 and 2010.

FIRST CLAIM FOR RELIEF

(Misappropriation and Threatened Misappropriation of Trade Secrets against Defendants RED F, Target Point, Roselli, Teng Li, Jason Li, Xu, and Epperly)

134. The allegations contained in paragraphs 1 through 133 of this complaint are realleged and incorporated herein by reference.

135. Defendants Teng Li, RED F, and Roselli used Bridgetree confidential information and trade secrets to establish RED F's Xian office and compete against

Bridgetree. Specifically and without limitation, Teng Li, RED F, and Roselli used compensation of employees, specific employees' knowledge of Bridgetree's proprietary systems and projects, vendor and customer information, and the methods of operations, set up (from India and Xian operations), Bridgetree's data mining and pre-mover knowhow, programs, source code are business and technical information of Bridgetree which derives independent, actual or potential commercial value from not being generally known or readily ascertainable to persons outside Bridgetree. This information is the subject of efforts by Bridgetree that are reasonable under the circumstances to maintain their secrecy.

136. The information taken by Teng Li and Jason Li from their Bridgetree computers and used by Teng Li and RED F to establish RED F's data mining and pre-mover services is business and technical information of Bridgetree which derives independent, actual or potential commercial value from not being generally known or readily ascertainable to persons outside Bridgetree. This information is the subject of efforts by Bridgetree that are reasonable under the circumstances to maintain their secrecy.

137. Upon information and belief, Defendants RED F, Target Point, Roselli, Teng Li, Jason Li, Xu, and Epperly have, and will continue to, misappropriate Bridgetree's trade secrets and will use them for their own benefit. Specifically and without limitation, Defendants have misappropriated employee, vendor and customer information, methods of operations, set up (from India and Xian operations), data mining and pre-mover know-how, programs, source code and used such information, along with the needs of such customers, vendors and employees, to improperly solicit employees and customers for themselves.

138. The information used by Defendants to establish Target Point and compete against Bridgetree is business and technical information of Bridgetree which derives independent, actual or potential commercial value from not being generally known or readily ascertainable to persons outside of Bridgetree. This information is the subject of efforts by Bridgetree that are reasonable under the circumstances to maintain their secrecy.

139. Upon information and belief, Defendants have, and will continue to, misappropriate Bridgetree's trade secrets and will use them for their own benefit or for third parties who are not entitled to access to such information. Specifically, Defendants have misappropriated employee, vendor and customer information, Bridgetree's pre-mover programs, source code, knowhow, and other data of Bridgetree's and used such information, along with the knowledge gained thereby of needs of such Bridgetree customers, vendors and employees, to improperly solicit employees and customers for themselves or to secure work from third parties competitive to Bridgetree.

140. Defendants' conduct constitutes the misappropriation and threatened misappropriation of Bridgetree's trade secrets and has and will proximately cause damage to Bridgetree for which it is entitled to recover pursuant to the North Carolina Trade Secrets Protection Act, N.C. Gen. Stat. § 66-152 through 157, and the common law.

141. Defendants' conduct is wrongful, willful and malicious. Accordingly, Bridgetree is entitled to recover from Defendants punitive damages, in addition to its actual damages and attorney's fees, pursuant to applicable statutes.

142. In addition to its recovery of monetary damages and because their actions have and will cause irreparable injury, Bridgetree is entitled to have Defendants' misappropriation, disclosure and use of Bridgetree's trade secrets enjoined by this Court; all such trade secrets, in tangible form, returned to Bridgetree; and all documents and things created from Bridgetree's trade secrets destroyed.

SECOND CLAIM FOR RELIEF

(Violation of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §§ 1962(c) and (d), Against Defendants Roselli, Teng Li, Jason Li, Xu, Epperly, and Scripter)

143. The allegations contained in paragraphs 1 through 142 of this complaint are realleged and incorporated herein by reference.

144. This claim for relief arises under the Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. §§ 1961 *et. seq.*, and is asserted against Defendants Roselli, Teng Li, Jason Li, Xu, Scripter and Epperly collectively the "RICO Defendants."

145. Defendant RED F is an enterprise engaged in activities in and affecting interstate commerce and foreign commerce within the meaning of an enterprise in 18 U.S.C. § 1961(4).

146. Defendant Target Point is an enterprise engaged in activities in and affecting interstate commerce and foreign commerce within the meaning of an enterprise in 18 U.S.C. § 1961(4).

147. The RICO Defendants, being persons within the meaning of 18 U.S.C. § 1961(3), and as persons associated with and employed by the enterprises alleged herein, conducted and participated in, directly and indirectly, the conduct of the affairs of said enterprises through a pattern of racketeering activity in violation of 18 U.S.C. § 1962(c).

148. The RICO Defendants, being persons within the meaning of 18 U.S.C. § 1961(3), engaged in a conspiracy to violate 18 U.S.C. § 1962(c), in violation of 18 U.S.C. § 1962(d), with the specific intent and expectation to injure Plaintiffs.

149. The predicate acts of racketeering activity engaged in by the RICO Defendants and those acting in concert with them or under their direction, include but are not limited to participation in a scheme to defraud by use of interstate wire (18 U.S.C. § 1343) as alleged herein.

150. Plaintiffs' businesses were injured by reason of these violations in that as a direct and proximate result of Defendants' acts, Plaintiffs suffered damages as alleged herein.

151. By reason of the Defendants' violations as specified above, Plaintiffs are entitled to three times their actual damages pursuant to 18 U.S.C. § 1964, with interest thereon from the date of loss and reasonable attorneys' fees.

THIRD CLAIM FOR RELIEF
(Unfair and Deceptive Trade Practices Against All Defendants)

152. The allegations contained in paragraphs 1 through 151 of this complaint are realleged and incorporated herein by reference.

153. Pursuant to N.C. Gen. Stat. §75-1.1, Defendants' conduct as set forth in this complaint constitutes an unfair method of competition and an unfair or deceptive act or practice in and affecting commerce, which has and will injure the goodwill and business of Bridgetree and has and will result in losses to it.

154. Accordingly, pursuant to N.C. Gen. Stat. §75-1.1 and §75-16, Bridgetree is entitled to recover from Defendants such damages as it may prove at trial and have those

damages trebled. Bridgetree is also entitled to recover its reasonable attorney's fees pursuant to N.C. Gen. Stat. §75-16.1.

FOURTH CLAIM FOR RELIEF
(Computer Trespass, N.C. Gen. Stat. § 14-458, Against Defendant Teng Li)

155. The allegations contained in paragraphs 1 through 154 of this complaint are realleged and incorporated herein by reference.

156. Pursuant to N.C. Gen. Stat. § 14-458, Teng Li's conduct as set forth in this complaint constitutes unauthorized use of a computer with the intent to erase and copy Bridgetree's computer data.

157. Teng Li's unlawful actions have caused significant injury to Bridgetree. Bridgetree is entitled to recover damages sustained and the costs of the suit pursuant to N.C. Gen. Stat. § 1-539.2A.

FIFTH CLAIM FOR RELIEF
(Computer Fraud and Abuse Act, 18 U.S.C. § 1030 et seq.,
Against Defendants RED F, Target Point and Teng Li)

158. The allegations contained in paragraphs 1 through 157 of this complaint are realleged and incorporated herein by reference.

159. Defendants have violated the Computer Fraud and Abuse Act, 18 U.S.C.§ 1030(a)(2)(C), by intentionally accessing a computer used for interstate commerce or communication, without authorization or by exceeding authorized access to such a computer, and by obtaining information from such a protected computer.

160. Defendants have violated the Computer Fraud and Abuse Act, 18 U.S.C. §1030(a)(4) by knowingly, and with intent to defraud Bridgetree, accessing a protected computer, without authorization or by exceeding authorized access to such a computer,

and by means of such conduct furthered the intended fraud and obtained one or more things of value.

161. Defendants have violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(B) by intentionally accessing a protected computer without authorization, recklessly causing damage to Bridgetree.

162. Defendants have violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(C) by intentionally accessing a protected computer without authorization, causing damage and loss to Bridgetree.

163. The computer system or systems that Defendants accessed as described above constitute a "protected computer" within the meaning of 18 U.S.C. § 1030(e)(2).

164. Bridgetree has suffered damage and loss by reason of these violations, including, without limitation, harm to Bridgetree's data, programs, and computer systems and other losses and damage in an amount to be proved at trial, but, in any event, in an amount well over $5000 aggregated over a one-year period.

165. Bridgetree is entitled to recover compensatory damages sustained pursuant to 18 U.S.C. § 1030(g).

166. Defendants' unlawful access to and theft from Bridgetree's computers also have caused Bridgetree irreparable injury. Unless restrained and enjoined, Defendants will continue to commit such acts. Bridgetree's remedy at law is not adequate to compensate it for these continuing injuries, entitling Bridgetree to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

SIXTH CLAIM FOR RELIEF
(Violation of Digital Millennium Copyright Act, 17 U.S.C. § 1201,
Against Defendant Teng Li and RED F)

167. The allegations contained in paragraphs 1 through 166 of this complaint are realleged and incorporated herein by reference.

168. Defendants Teng Li and RED F have violated and continue to violate the Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(1)(A), by circumventing the technological measures that effectively control access to Bridgetree's copyright-protected Bridgetree National Database.

169. Upon information and belief, Teng Li gained access to the Bridgetree National Database interface and reinstated his username's access and changed his password to circumvent the username and password authentication system that controls access to the Bridgetree National Database interface.

170. Upon information and belief, Bob Yuan, acting under RED F's direction or control, gained access to the Bridgetree National Database server using a username and password that Bob Yuan and RED F were not authorized to use, thus circumventing the authentication system that controls access to the Bridgetree National Database interface.

171. Bridgetree has been and continues to be damaged by Defendants Teng Li's and RED F's actions and conduct. Further, if Teng Li and RED F are not enjoined and are allowed to continue this present conduct, Bridgetree will suffer irreparable injury, which cannot be adequately compensated by monetary damages. Bridgetree is therefore entitled to injunctive relief as provided by 17 U.S.C. 1203(b).

SEVENTH CLAIM FOR RELIEF
(Conversion Against RED F, Teng Li, and Mali Xu)

172. The allegations contained in paragraphs 1 through 171 of this complaint are realleged and incorporated herein by reference.

173. RED F, through its agent Mali Xu, wrongfully converted Bridgetree property, including Bridgetree Xian's accounting books and ledgers and a computer belonging to Bridgetree, to RED F's own use and enjoyment, thus depriving Bridgetree of its property. RED F engaged in these activities with the intent to permanently deprive Bridgetree of the use of its property.

174. Teng Li, wrongfully converted Bridgetree property, including files taken from computers belonging to Bridgetree, for his and RED F's own use and enjoyment, thus depriving Bridgetree of its property. Teng Li engaged in these activities with the intent to permanently deprive Bridgetree of the use of its property.

175. RED F's, Teng Li's, and Mali Xu's unauthorized assumption and exercise of rights of ownership have been to the exclusion of the ownership rights of Bridgetree.

176. RED F's, Teng Li's, and Mali Xu's conduct is wrongful, willful and malicious. Accordingly, Bridgetree is entitled to recover from Defendants punitive damages, in addition to its actual damages and attorney's fees, pursuant to applicable statutes.

177. RED F's, Teng Li's, and Mali Xu's conversion of Bridgetree's property has caused and threatens to continue to cause Bridgetree to suffer irreparable injury, for which adequate redress may not be had at law. Thus, for such conversion, Bridgetree is entitled to injunctive relief, including a preliminary injunction and permanent injunction.

EIGHTH CLAIM FOR RELIEF
(Civil Conspiracy Against All Defendants)

178. The allegations contained in paragraphs 1 through 177 of this complaint are realleged and incorporated herein by reference.

179. Upon information and belief, Defendants, including Scripter, acted together, in concert, to commit one or more of the acts complained of herein: i.e., misappropriation of trade secrets, unfair and deceptive trade practices, conversion, and computer trespass.

180. Upon information and belief, Defendants had an agreement, express or implied, to undertake these acts in order to injure Bridgetree and to benefit RED F.

181. The acts complained of herein constitute overt acts in furtherance of the conspiracy.

182. Defendants are jointly and severally liable for each others' bad acts done in furtherance of the conspiracy.

183. As a result of the foregoing actions, Bridgetree has incurred damages in an amount greater than $10,000.00, and is entitled to punitive damages for willful and malicious misappropriation.

NINTH CLAIM FOR RELIEF
(Breach of Fiduciary Duty Against Teng Li)

184. The allegations contained in paragraphs 1 through 183 of this complaint are realleged and incorporated herein by reference.

185. Teng Li held a position of trust and confidence as a Vice President of Bridgetree and a member of Two Bit Dog. Teng Li owed various fiduciary duties and obligations including, but not limited to, duties of loyalty and good faith, the duty to disclose fully and truthfully all matters pertaining to membership and the duty to protect and preserve

Bridgetree's and Two Bit Dog's trade secrets, confidential and proprietary information and customer and employee relationships, and the duty to not prefer his own interests over the interests of Bridgetree and Two Bit Dog.

186. Li, in working with a competitor, RED F, to establish an office in Xian and crippling Bridgetree by his departure and destruction of data, violated the duties Teng Li owed to Bridgetree and Two Bit Dog as a result of his position as Vice President of Bridgetree and his role as a member of Two Bit Dog, including, specifically, duties of loyalty, trust and confidentiality he owed to Bridgetree and Two Bit Dog.

187. As a result of his breach of fiduciary duties, Bridgetree and Two Bit Dog are entitled to recover from Teng Li such compensatory and punitive damages for willfully, maliciously and consciously disregarding the rights of Bridgetree and Two Bit Dog as will be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectively pray that:

1. The Court order that Roselli, Epperly, Teng Li, Jason Li, Mali Xu, Scripter, Target Point, RED F, and any employee currently employed with RED F or Target Point, return to Bridgetree all of its confidential information and trade secrets that are in tangible form and destroy any other documents created by any of them from the trade secrets of Bridgetree or its vendors or customers;
2. The Court enter an Order pursuant to N.C. Gen. Stat. §66-154(a) enjoining Defendants from continuing to use Bridgetree's trade secrets and confidential information, including, without limitation, Bridgetree's customer, employee and

vendor information, Bridgetree's pre-mover and print marketing on-demand data and process, and from continuing to compete with Bridgetree unfairly;

3. The Court enter judgment against Defendants for their violation of the North Carolina Trade Secrets Protection Act, in the amount of damages as will be proven at trial pursuant to N.C. Gen. Stat. § 66-154(a), as well as punitive damages and attorneys' fees for Defendants' willful and malicious trade secret misappropriation, pursuant to N.C. Gen. Stat. § 66-154(c) and (d);
4. The Court enter judgment against Defendants Roselli, Teng Li, Jason Li, Mali Xu, Mark Epperly, and Elton Scripter, for their violation of the Racketeer Influenced and Corrupt Organizations Act, in the amount of damages as will be proven at trial, as well as treble damages, costs, and attorney's fees, pursuant to 18 U.S.C. § 1964(c);
5. The Court enter judgment against Defendants for their violation of the North Carolina Unfair and Deceptive Trade Practices Act, in the amount of damages as will be proven at trial, as well as treble damages, pursuant to N.C. Gen. Stat. § 75-16, and attorney's fees and costs, pursuant to N.C. Gen. Stat. § 75-16.1;
6. The Court enter judgment against Teng Li individually for his acts of computer trespass, in the amount of damages as will be proven at trial, including costs, pursuant to N.C. Gen. Stat. § 1-539.2A;
7. The Court enter judgment against Defendants RED F, Target Point, and Teng Li, for their violation of the Computer Fraud and Abuse Act, in the amount of damages as will be proven at trial, pursuant to 18 U.S.C. § 1964(c);

8. The Court enter an Order pursuant to 17 U.S.C. § 1203(b)(1), enjoining Defendants from any further circumvention of any technological measure that effectively controls access to a copyright-protected work owned by Bridgetree and/or Two Bit Dog, or any conduct that otherwise violates the Digital Millennium Copyright Act;
9. The Court enter judgment against Defendants RED F and Teng Li, for their violation of the Digital Millennium Copyright Act, in the amount of damages as will be proven at trial, pursuant to 17 U.S.C. § 1203(c), as well as costs, pursuant to 17 U.S.C. § 1204(b)(4), and attorney's fee, pursuant to 17 U.S.C. § 1203(b)(5).
10. The Court enter judgment against Defendants for their acts of conversion and conspiracy, and for compensatory and punitive damages as will be proven at trial;
11. The Court enter judgment against Defendant Teng Li for his breach of fiduciary duty, and for compensatory and punitive damages as will be proven at trial;
12. The Court grant Plaintiffs such other and further relief as it deems just and appropriate.

Plaintiffs hereby demand a trial by jury on all issues so triable.

Date: May 18, 2010

s/ J. Mark Wilson
J. Mark Wilson
N.C. State Bar No. 25763
Kathryn G. Cole
N.C. State Bar No. 39106
Moore & Van Allen PLLC
Suite 4700
100 North Tryon Street
Charlotte, NC 28202-4003
Telephone (704) 331-1000
Facsimile (704) 339-5981
Email: markwilson@mvalaw.com
Email: katecole@mvalaw.com

Steven C. Schroer
Fitch, Even, Tabin & Flannery
1942 Broadway, Suite 213
Boulder, Colorado 80302
Telephone: (303) 402-6966
Facsimile: (303) 402-6970
Email: scschr@fitcheven.com

Edward W. Gray
Christian R. Eriksen
Fitch, Even, Tabin & Flannery
One Lafayette Center, Suite 750S
1120 20th Street, NW
Washington, DC 20036
Telephone: (202) 419-7000
Facsimile: (202) 419-7007
Email: egray@fitcheven.com
Email: ceriksen@fitcheven.com

Attorneys for Plaintiffs Bridgetree, Inc. and Two Bit Dog, LLC